AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

Your Affiant, Jonathan Lobus, being first duly sworn, deposes and states as follows:

1. I am a Special Agent with the United States Secret Service (USSS), and have been since August 2015. I am a graduate of the Federal Law Enforcement Training Center Basic Criminal Investigator Training Program and the United States Secret Service Special Agent Training Course. I am currently assigned to the Criminal Squad of the Baltimore Field Office and have participated in numerous financial crime investigations to include counterfeit, identity theft, check fraud, wire fraud, and bank fraud cases. I have conducted physical surveillances, executed search warrants, reviewed computer and bank records, and secured other relevant information using other investigative techniques. I have also completed the Basic Investigation of Computers and Electronic Crimes Program (BICEP). Prior to my position as Special Agent with the Secret Service, I spent seven years as a Uniformed Division Officer with the Secret Service.

2. This affidavit is submitted in support of an application for the issuance of a search warrant for the following Subject Electronic Device:

a.) ZTE Cell Phone: Z981, Serial: #329766801955

The Subject Electronic Device is presently held by the USSS at 100 South Charles Street, Baltimore, MD 21201 and is also described in Attachment A.

3. Based on the investigation to date, I submit that there is probable cause to believe that a search of the Subject Electronic Device will uncover evidence, fruits, and/or instrumentalities of the following offenses: Bank Fraud Conspiracy, violation of 18 U.S.C. § 1349; Bank Fraud, in violation of 18 U.S.C. § 1344; and Aggravated Identity Theft, in violation of 18 U.S.C. § 1028A (collectively referred to as the "TARGET OFFENSES").

4. Federal law enforcement and intelligence officials have participated in this investigation and have witnessed many of the facts and circumstances described by me herein. The information set forth in this affidavit is based on my review of documents, or reliable information provided to me by other law enforcement personnel, banking institution investigators, and other suspects involved in the investigation. I am setting forth only those facts and

circumstances necessary to establish probable cause for the issuance of the requested search warrant. However, I have not omitted any fact that might tend to defeat a finding of probable cause. Unless otherwise indicated, all written and oral statements referred to herein are set forth in substance and in part, rather than verbatim.

Probable Cause

5. Since June 2013, USSS-Baltimore Field Office, Howard County, Maryland Police Department, Maryland National Capital Park Police, Baltimore County Police, Anne Arundel County Police, and the United States Attorney's Office for the District of Maryland, have been involved in the investigation of the Felony Lane Gang (also referred to as "FLG") and its illegal activity occurring in and around the greater Baltimore/Washington metropolitan area and elsewhere.

a. The term "Felony Lane Gang" is used to identify an organization originating in Florida and operating multiple theft crews, which have consistent methods of conducting criminal activity across several states. These theft crews share group leaders and street level personnel.

b. The name "Felony Lane Gang" arises from the group's general use of the bank drive-thru lane furthest from the tellers when trying to cash stolen checks or use stolen bank cards with stolen IDs. This outside lane is referred to as "Felony Lane" because use of the far lane makes it difficult for bank tellers to see whether the person in the car matches the picture on the identification being presented to the bank. The gang has even brought wigs and glasses to help those cashing stolen checks to look more like the individuals pictured in the stolen IDs.

c. Members of the "Felony Lane Gang" are targeting victims who leave their personal items, such as purses and personal bags, wallets, and diaper bags in their parked cars when going to places like the gym, park, daycare, and church. Members of the "Felony Lane Gang" then break into these parked vehicles to gain access to these personal items so they can use these items, such as credit cards, ATM cards, and checks. These criminals have been observed and video-taped cruising parking lots looking for target

vehicles. When one is selected they break the vehicle's window and quickly snatch purses and valuables. The "smash and grab" can take as few as 10-15 seconds. The "Felony Lane Gang" uses sophisticated methods, such as counter surveillance and look-outs. These thefts from vehicles, accompanied by the fraudulent use of victims' personal information, identification, and banking documents have occurred throughout the United States.

d. Members of the conspiracy, generally in teams of a driver and a passenger posing as the victim, travel to banks to cash the checks stolen from victims. Other members of the conspiracy are either in another car parked nearby so they can watch both the transaction and look out for police, or they are crouched down behind the front seat. As an example of a typical transaction, a check stolen from Victim One will be made payable to Victim Two and cashed at Victim Two's bank using Victim Two's Driver's License and debit card. A member of the conspiracy poses as Victim Two in the transaction. The individuals who conduct these transactions posing as victims are called "faces."

e. On October 27, 2015, thirteen individuals involved in the Felony Lane Gang were indicted by a federal grand jury sitting in the District of Maryland based on FLG activities in occurring in Maryland and elsewhere. The case was entitled *United States of America v. Theodore Pittman, et al.*, Criminal No. MJG-15-0565 and the individuals were charged with bank fraud conspiracy, bank fraud and aggravated identity theft.

6. Members of law enforcement have spoken with numerous FLG members since 2013. FLG members have stated that members of FLG would regularly communicate via cellular phones in order to conduct surveillance, lookouts, recruitment, and communicate with other FLG teams. Several FLG members have reported that Kevin WILLIAMS serves as a leader or organizer or manager of FLG who has been responsible for car break ins to obtain checks and identification that are used in fraudulent check cashing and also leads teams of cashers that actually cash the fraudulent checks.

7. For example, Cooperator 1, an indicted co-conspirator in the case entitled *United States of America v. Theodore Pittman, et al.*, described above who worked with Kevin WILLIAMS, stated that WILLIAMS actively participated in FLG as a co-manager. Cooperator

1 stated s/he would routinely travel back to Florida; however, Kevin WILLIAMS would stay in Maryland to manage their FLG crew. Cooperator 1stated WILLIAMS told him about breaking into a car and surprising a person in the car. Video surveillance shows Kevin WILLIAMS attempting to break into a Toyota Avalon at Kenwood Country Club in Bethesda, Maryland on May 29, 2013. In the video, WILLIAMS can be seen immediately running away. The woman who was in the backseat of that vehicle reported to police about the break in and gave a general description of the perpetrator.

8. Cooperator 2, an indicted co-conspirator who worked with Kevin WILLIAMS, stated s/he was recruited by Kevin WILLIAMS into FLG. On June 2, 2013, victim C.A.'s Dodge Caravan was broken into at the Knights of Columbus Building in College Park, MD. C.A's purse was stolen from that vehicle. On July 5, 2013, victim K.S.'s Toyota Highlander was broken into at Meadowlane Park in Howard County. The driver's side window was broken and K.S.'s wallet was stolen, along with her checkbook, credit cards, and debit cards. Bank surveillance images show Cooperator 2, along with another co-conspirator, cashing a check number 382 at the SECU in Owings Mills. Check 382 was from K.S.'s account and made out to C.A. Neither K.S. nor C.A. consented to their vehicles being broken into, nor did they consent to the use of their identities being used to commit fraud against the bank. Cooperator 2 advised that s/he traveled to Maryland from Florida one time to participate in fraudulent check cashing activity, including the fraudulent check cashing described in this paragraph, and that Kevin WILLIAMS was in Maryland for that trip and helped supervise the team of "faces" that included Cooperator 2.

8. Cooperator 3 and Cooperator 4, two more indicted co-conspirators who worked with Kevin WILLIAMS, stated they participated in FLG activity with Kevin WILLIAMS in Maryland. Bank surveillance images show Cooperator 3 and Cooperator 4 cashing checks at the PNC in Annapolis, Maryland on January 18, 2013. Cooperator 3 and Cooperator 4 cashed check 2702 from J.M's account and made payable to E.K. J.M. and E.K. did not consent to any of these transactions.

9. Cooperator 5, another indicted co-conspirator, stated s/he participated in FLG activity with Kevin WILLIAMS. Bank surveillance images show Cooperator 5 cashing a check at the Edgewood Branch of Aberdeen Proving Ground Federal Credit Union on March 29, 2013. Cooperator 5 also cashed check number 1049 for the Community Bank account ending in 1036

and belonging to victim J.T. J.T. did not agree to the break in of her vehicle nor did she consent to the use of her identities to commit fraud against the bank.

10. Cooperator 6, another indicted co-conspirator, has advised that s/he participated in FLG activity with Kevin WILLIAMS. Jail calls between Cooperator 6 and Kevin WILLIAMS corroborate that WILLIAMS actively participated in FLG.

11. Based on this evidence described above and other evidence, on November 29, 2017, an arrest warrant was issued for Kevin WILLIAMS after a federal grand jury in the District of Maryland returned an Indictment charging Williams with one count of bank fraud conspiracy, in violation of 18 U.S.C. § 1349; three counts of bank fraud, in violation of 18 U.S.C. § 1344; and four counts of aggravated identity theft, in 18 U.S.C. § 1028A.

12. On December 6, 2017, WILLIAMS was arrested in Fort Lauderdale, Florida on the arrest warrant issued on November 29, 2017. A search incident to arrest of WILLIAMS led to the recovery of the Subject Electronic Device.

Request to Search

13. Your Affiant knows through training, knowledge and experience that individuals who conspire to commit bank fraud and identity theft, in the manner described previously in this Affidavit, require a considerable amount of communication between themselves and other conspirators. Specifically, I know that such conspirators use cellular telephones and/or computers to communicate; and that these devices can serve to log and record evidence of and fruits of criminal activities. Additionally, I know that cellular telephones are utilized for the purposes other than making phone calls, including sending and receiving SMS or "text" messages, as well as sending or receiving emails. I also know that the information is often stored in the memory of cellular telephones for a period of time.

14. Information provided by cooperating defendants that confirms the members of the conspiracy routinely used cell phones to communicate and conspire during the course of the conspiracy and often carried and used multiple cell phones.

15. Based on my training, experience, and my participation in other investigations your Affiant knows the following:

a. Persons involved in identity theft crimes keep and maintain records of their various activities and utilize electronic storage media devices to store the records listed above and that these records can be stored and maintained for a significant period of time.

b. Persons involved in identity theft crimes utilize cellular telephones, pagers, and other electronic communication devices to facilitate illegal transactions. In this case cooperators all describe being on the phone with their FLG managers while conducting transactions. The electronically stored information on these devices is of evidentiary value in identifying other members of the conspiracy and establishing the relationship between these individuals.

16. In your Affiant's experience, as well as the common experience of any user of cellular phones, many occupants have free access to the various areas inside a residence and often have property located throughout the residence. Cellular phones, by their very nature, are portable devices and as a result are routinely placed in temporary locations within a dwelling by the users. Further, it is not possible to know the telephone number of a cellular phone simply by viewing the outside of the phone. Rather, at the very least, a cursory search of the cellular phone must be conducted to determine who the true user(s) of the cellular phone are.

17. For these reasons, the stored text messages and stored telephone numbers, names, addresses, voice mail messages, and other electronically stored data are evidence of the TARGET OFFENSES. Therefore, your Affiant seeks permission to search the Subject Electronic Device for telephone numbers, names, addresses, email addresses, opened and unopened voice mail messages, text messages, email, communications, photographs, financial records, money transfer records, travel records, and any other documents relevant to the investigation.

18. Accordingly, your Affiant respectfully requests that a search warrant for the Subject Electronic Device be issued, authorizing the search of the Subject Electronic Device, which are listed on attachment A, for call logs, contacts, calendars, GPS, or location information, voice messages, text or SMS messages, email messages, photographs, money transfer records, financial records, travel records or any other documents or files which are evidence of the violations identified above. The search shall be conducted pursuant to the protocol detailed in Attachment B.

17-3484 BPG

19. Furthermore, insofar as the Subject Electronic Devices are in the custody of agents of the United States Secret Service, your Affiant submits there is reasonable cause to authorize the search warrant to be executed at any time of day or night.

Conclusion

20. Based on the proceeding information, your Affiant asserts that there is probable cause to believe that evidence relating to the crimes of Bank Fraud Conspiracy in violation of Title 18, USC 1349; Bank Fraud in violation of Title 18, USC 1344; and Aggravated Identity Theft in violation of Title 18, USC 1028A will be found in the Subject Electronic Device currently being held by the United States Secret Service at 100 South Charles Street, Baltimore, Maryland 21201.

Jonathan Lobus
Special Agent
United States Secret Service
Baltimore Field Office

Subscribed and sworn to before me this 21st day of December 2017.

Beth P. Gesner
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A 17-3484 BPG

ITEMS TO BE SEIZED AND SEARCHED

a.) a ZTE Cell Phone: Z981, Serial: #329766801955, which is presently held by the USSS at 100 South Charles Street, Baltimore, MD 21201

17-3484 BPG

ATTACHMENT B

Description of Items to be Seized

This warrant authorizes the search of electronically stored information and other documents related to the item listed on Attachment A for call logs, contacts, calendars, GPS or location information, opened or unopened voice messages, opened or unopened text or SMS messages, opened or unopened email messages, photographs, money transfer records, financial records, travel records or any other documents or files which are evidence of Bank Fraud Conspiracy in violation of Title 18, USC 1349; Bank Fraud in violation of Title 18, USC 1344; and Aggravated Identity Theft in violation of Title 18, USC 1028A.

Due to the possibility that the files examined pursuant to the warrant will include information that is beyond the scope of what the United States has demonstrated the existence probable cause to search for, the search shall be conducted in a manner that will minimize to the greatest extent possible the likelihood that files or other information will be viewed for which there is no probable cause to search.

While this protocol does not prescribe the specific search protocol to be used, it does contain limitations to what government investigators may view during their search, and the searching investigators shall be obligated to document the search methodology used in the event there is a subsequent challenge to the search that was conducted, pursuant to the following protocol:

With respect to the search of any digitally/electronically stored information that is seized pursuant to this warrant and described in Attachment A hereto, the search procedure shall include such reasonably available techniques designed to minimize the chance that the government investigators conducting the search will view information that is beyond the scope for which probable cause exists.

The following list of techniques is a non-exclusive list which illustrates the types of search methodology that may avoid an overbroad search, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein:

a. Use of search methodology to conduct and examination of all the data contained in such hardware, software, and/or memory storage devices to determine whether that data falls within the items to be seized as set forth herein by specific data ranges, names of individuals, or organizations;
b. Searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein;
c. Physical examination of the storage device, including digitally surveying various file directories and the individual files they contain to determine whether they include data falling within the list of items to be seized as set forth herein;
d. Opening or reading portions of files that are identified as a result of conducting digital search inquiries in order.